FIG. 1

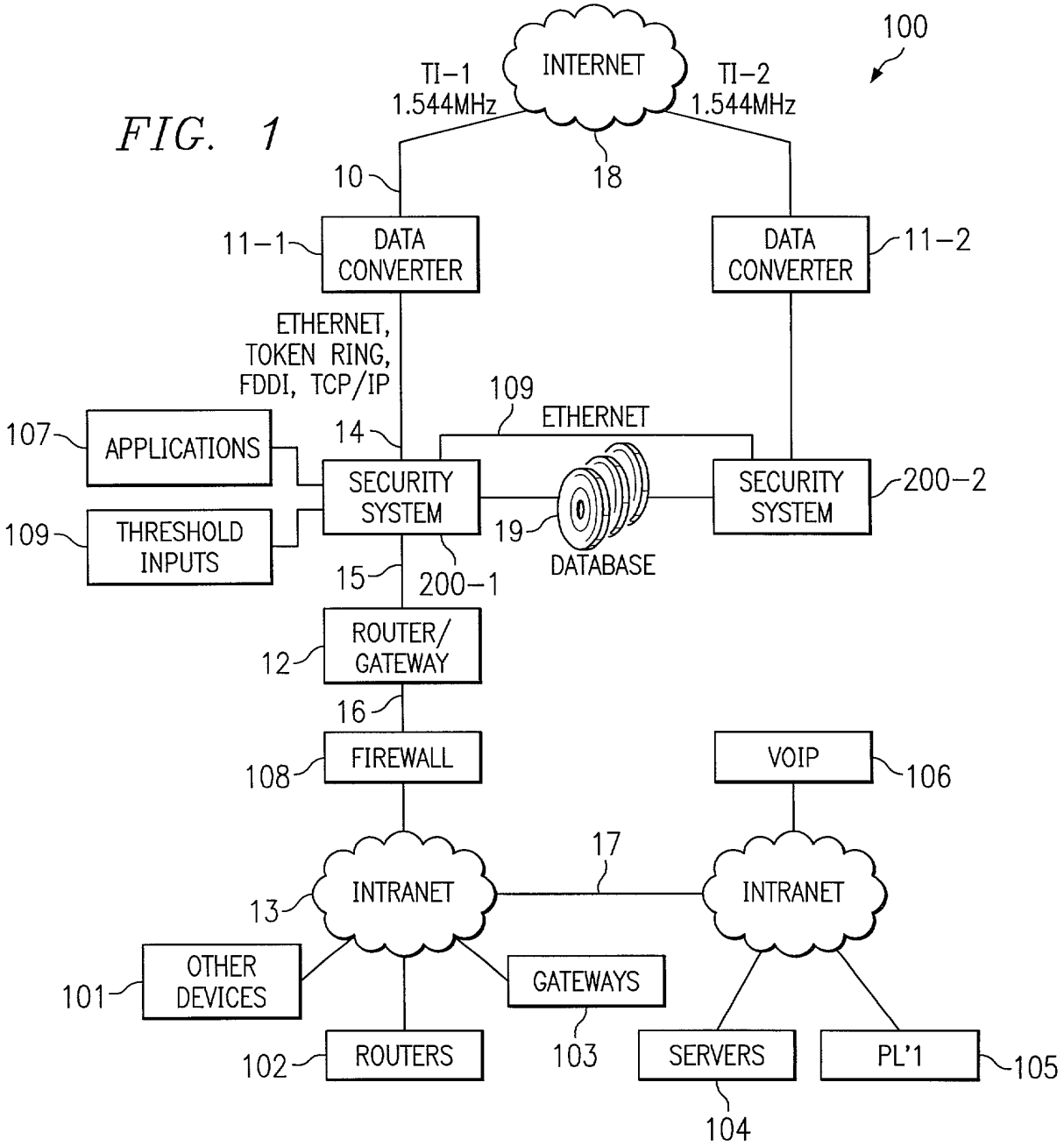
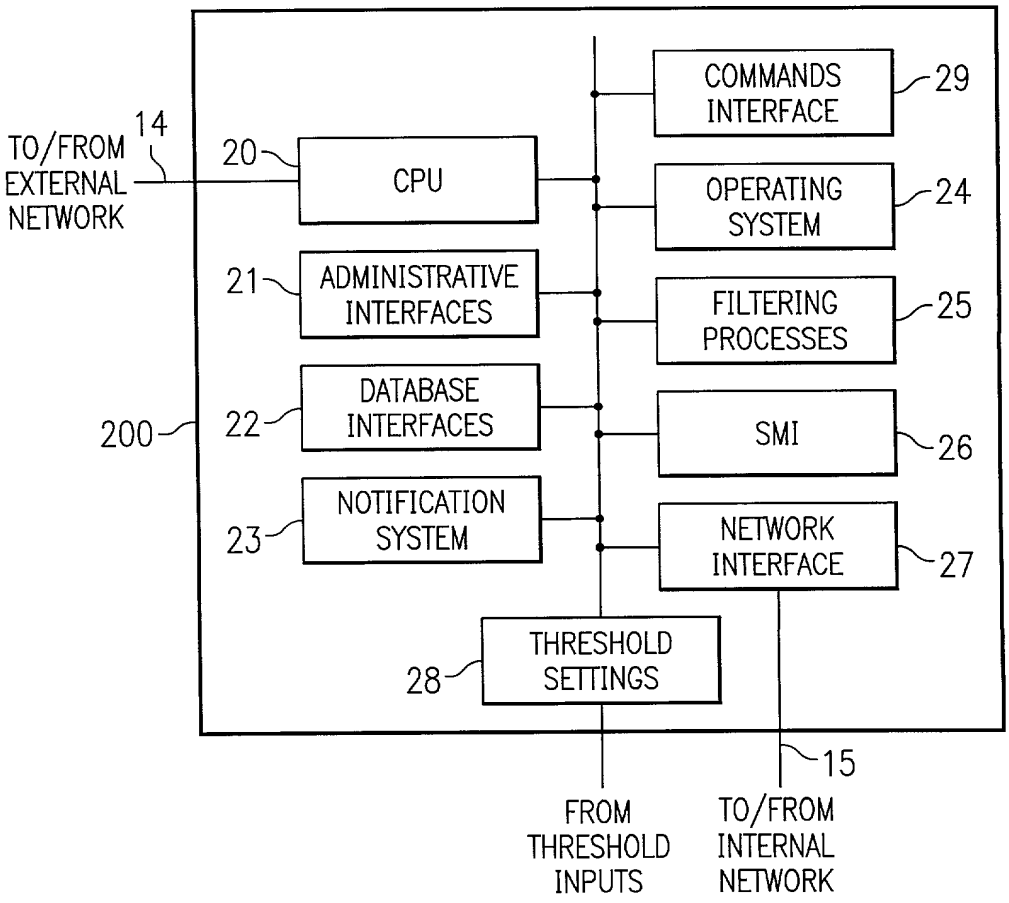

100
INTERNET
TI-1
1.544MHz
TI-2
1.544MHz
18
10
11-1
DATA
CONVERTER
DATA
CONVERTER
11-2
ETHERNET,
TOKEN RING,
FDDI, TCP/IP
109
ETHERNET
107
APPLICATIONS
14
SECURITY
SYSTEM
SECURITY
SYSTEM
200-2
109
THRESHOLD
INPUTS
19
DATABASE
15
200-1
ROUTER/
GATEWAY
12
16
FIREWALL
108
VOIP
106
17
INTRANET
INTRANET
13
OTHER
DEVICES
101
GATEWAYS
ROUTERS
102
103
SERVERS
PL'1
105
104

FIG. 2


TO/FROM EXTERNAL NETWORK
14
20
CPU
21
ADMINISTRATIVE INTERFACES
22
DATABASE INTERFACES
200
23
NOTIFICATION SYSTEM
28
THRESHOLD SETTINGS
COMMANDS INTERFACE
29
OPERATING SYSTEM
24
FILTERING PROCESSES
25
SMI
26
NETWORK INTERFACE
27
15
FROM THRESHOLD INPUTS
TO/FROM INTERNAL NETWORK

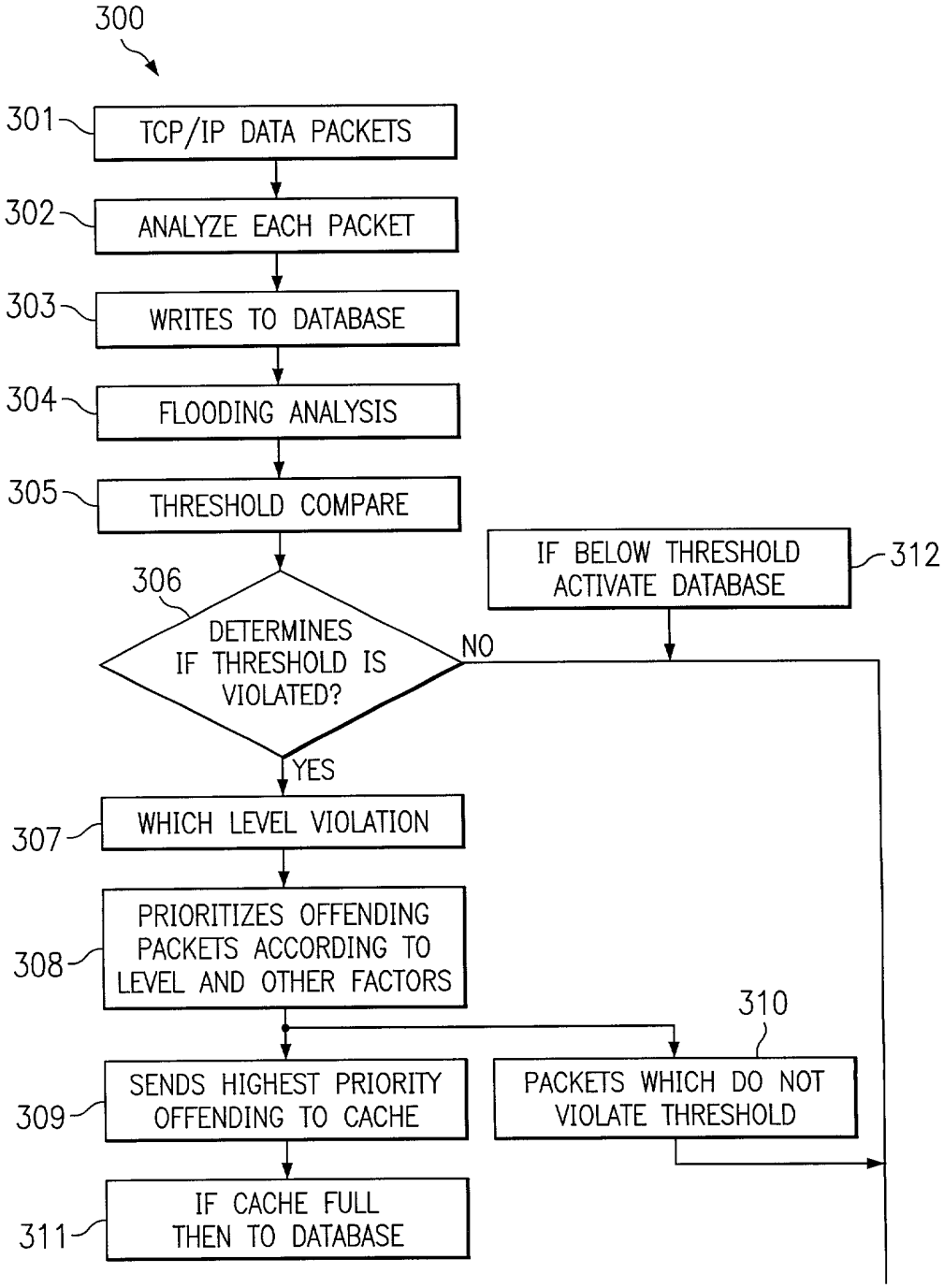

300
301
TCP/IP DATA PACKETS
302
ANALYZE EACH PACKET
303
WRITES TO DATABASE
304
FLOODING ANALYSIS
305
THRESHOLD COMPARE
306
DETERMINES IF THRESHOLD IS VIOLATED?
NO
YES
IF BELOW THRESHOLD ACTIVATE DATABASE
312
307
WHICH LEVEL VIOLATION
308
PRIORITIZES OFFENDING PACKETS ACCORDING TO LEVEL AND OTHER FACTORS
310
309
SENDS HIGHEST PRIORITY OFFENDING TO CACHE
PACKETS WHICH DO NOT VIOLATE THRESHOLD
311
IF CACHE FULL THEN TO DATABASE

FIG. 3

FIG. 4

0	1	2	3	4	5	6
MAIN POSIX PTS 2	IP1	CRUNCH	DETER CHOKE	WISH SUM LOWER	2 DATABASE FILTERS	SYNCH SHARED RESOURCES

FIG. 5

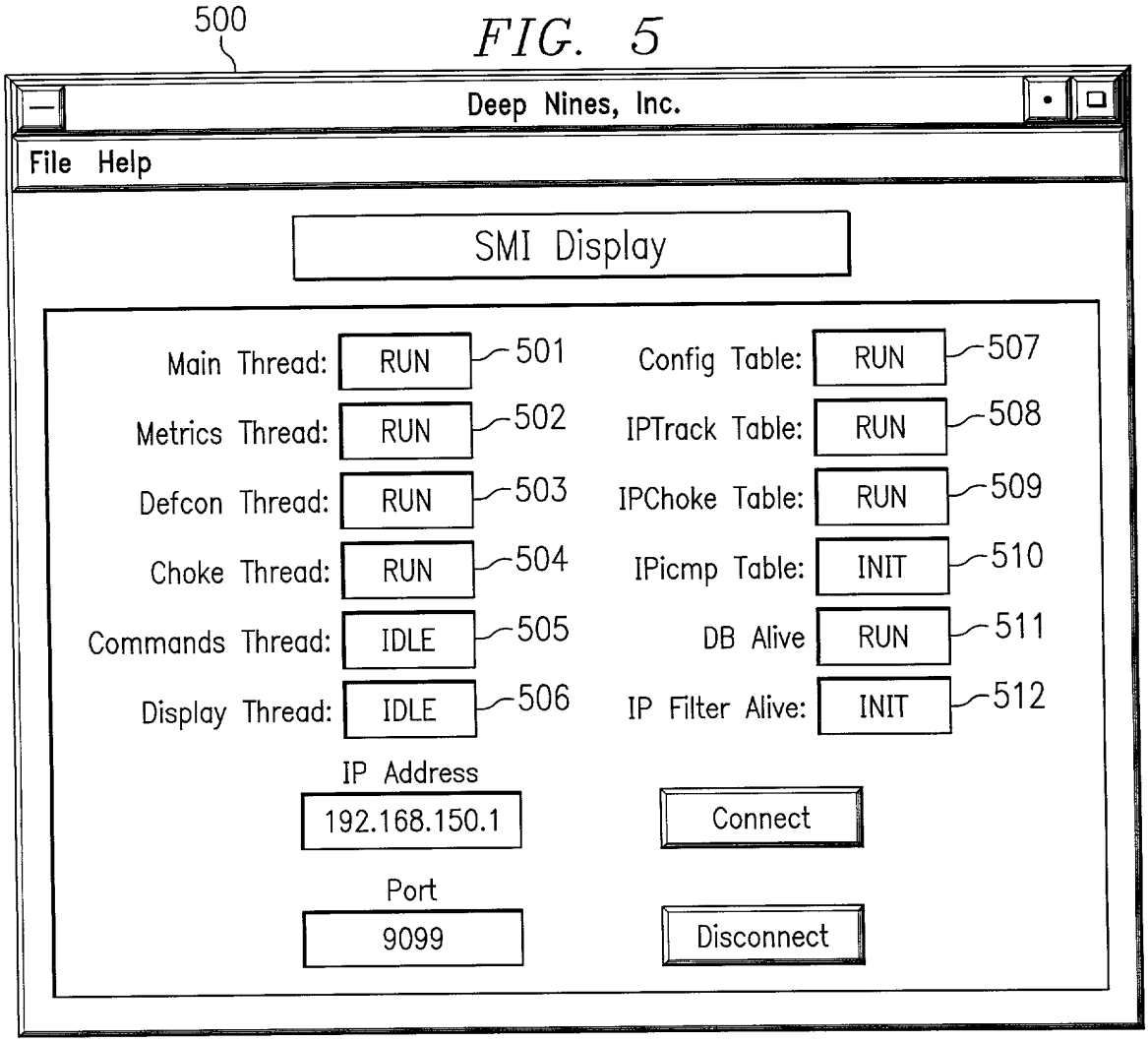
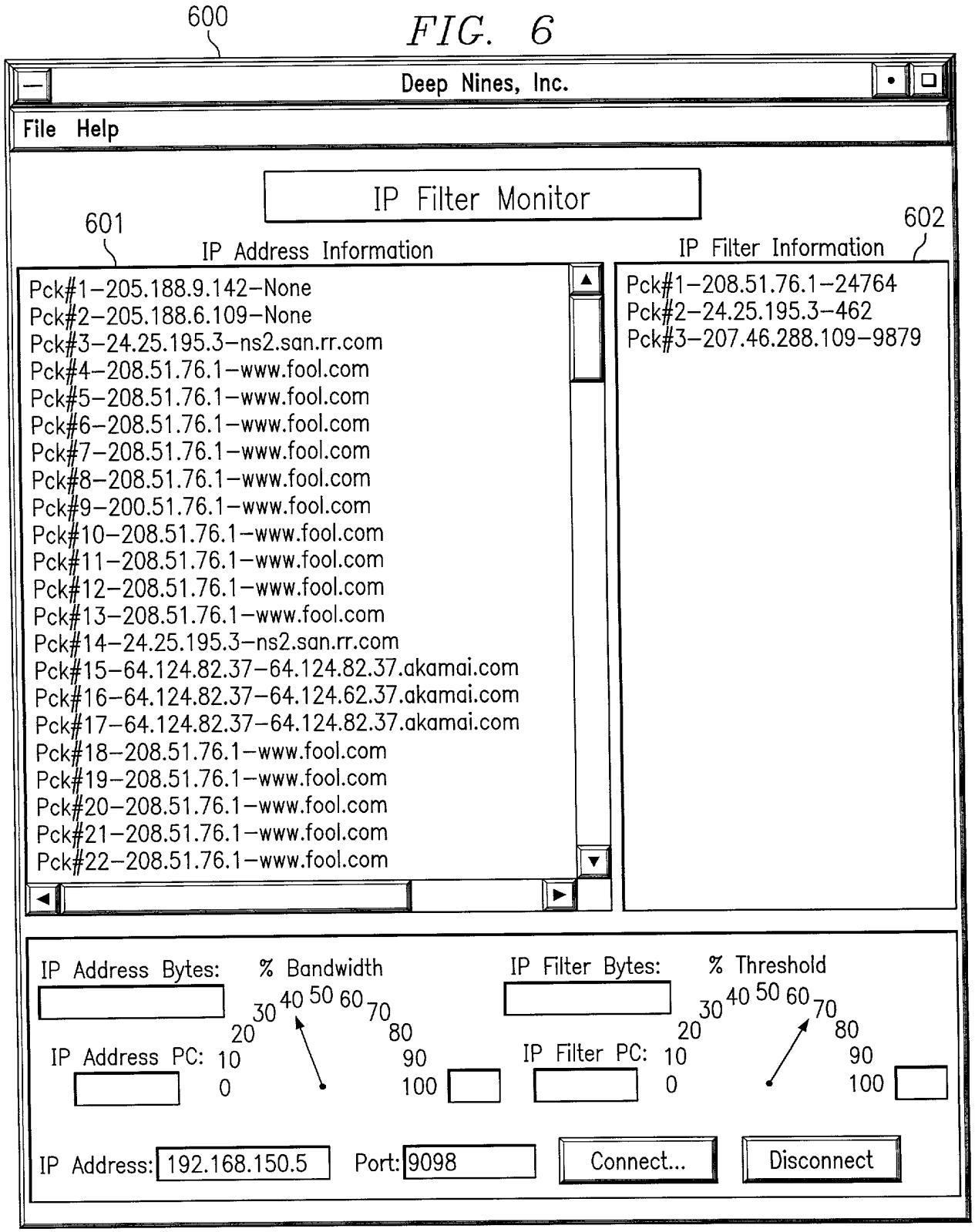


FIG. 6


600
Deep Nines, Inc.
File Help
IP Filter Monitor
601
IP Address Information
602
IP Filter Information
Pck#1-205.188.9.142-None
Pck#2-205.188.6.109-None
Pck#3-24.25.195.3-ns2.san.rr.com
Pck#4-208.51.76.1-www.fool.com
Pck#5-208.51.76.1-www.fool.com
Pck#6-208.51.76.1-www.fool.com
Pck#7-208.51.76.1-www.fool.com
Pck#8-208.51.76.1-www.fool.com
Pck#9-200.51.76.1-www.fool.com
Pck#10-208.51.76.1-www.fool.com
Pck#11-208.51.76.1-www.fool.com
Pck#12-208.51.76.1-www.fool.com
Pck#13-208.51.76.1-www.fool.com
Pck#14-24.25.195.3-ns2.san.rr.com
Pck#15-64.124.82.37-64.124.82.37.akamai.com
Pck#16-64.124.82.37-64.124.62.37.akamai.com
Pck#17-64.124.82.37-64.124.82.37.akamai.com
Pck#18-208.51.76.1-www.fool.com
Pck#19-208.51.76.1-www.fool.com
Pck#20-208.51.76.1-www.fool.com
Pck#21-208.51.76.1-www.fool.com
Pck#22-208.51.76.1-www.fool.com
Pck#1-208.51.76.1-24764
Pck#2-24.25.195.3-462
Pck#3-207.46.288.109-9879
IP Address Bytes:
% Bandwidth
0 10 20 30 40 50 60 70 80 90 100
IP Address PC:
IP Filter Bytes:
% Threshold
0 10 20 30 40 50 60 70 80 90 100
IP Filter PC:
IP Address: 192.168.150.5
Port: 9098
Connect...
Disconnect

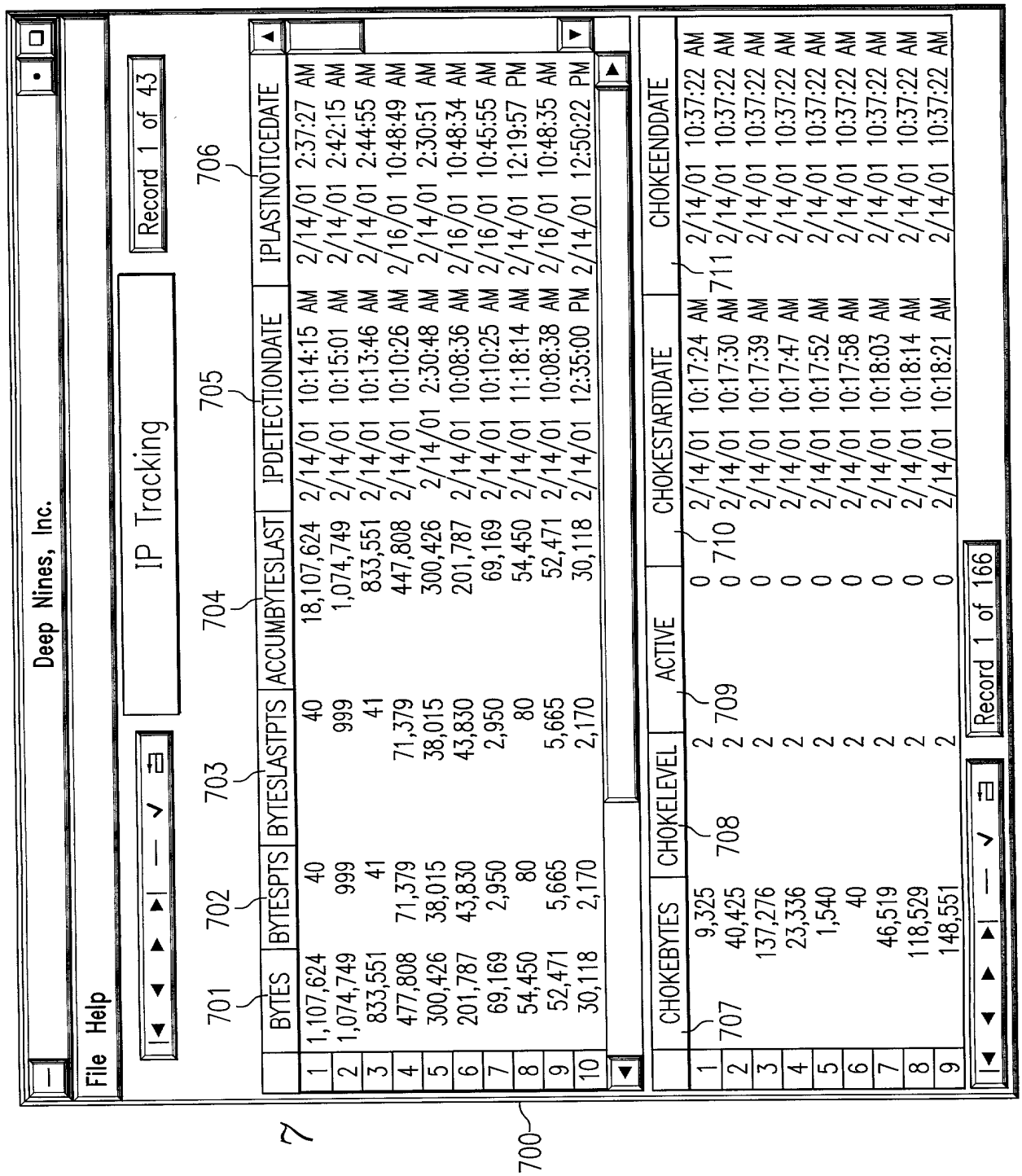
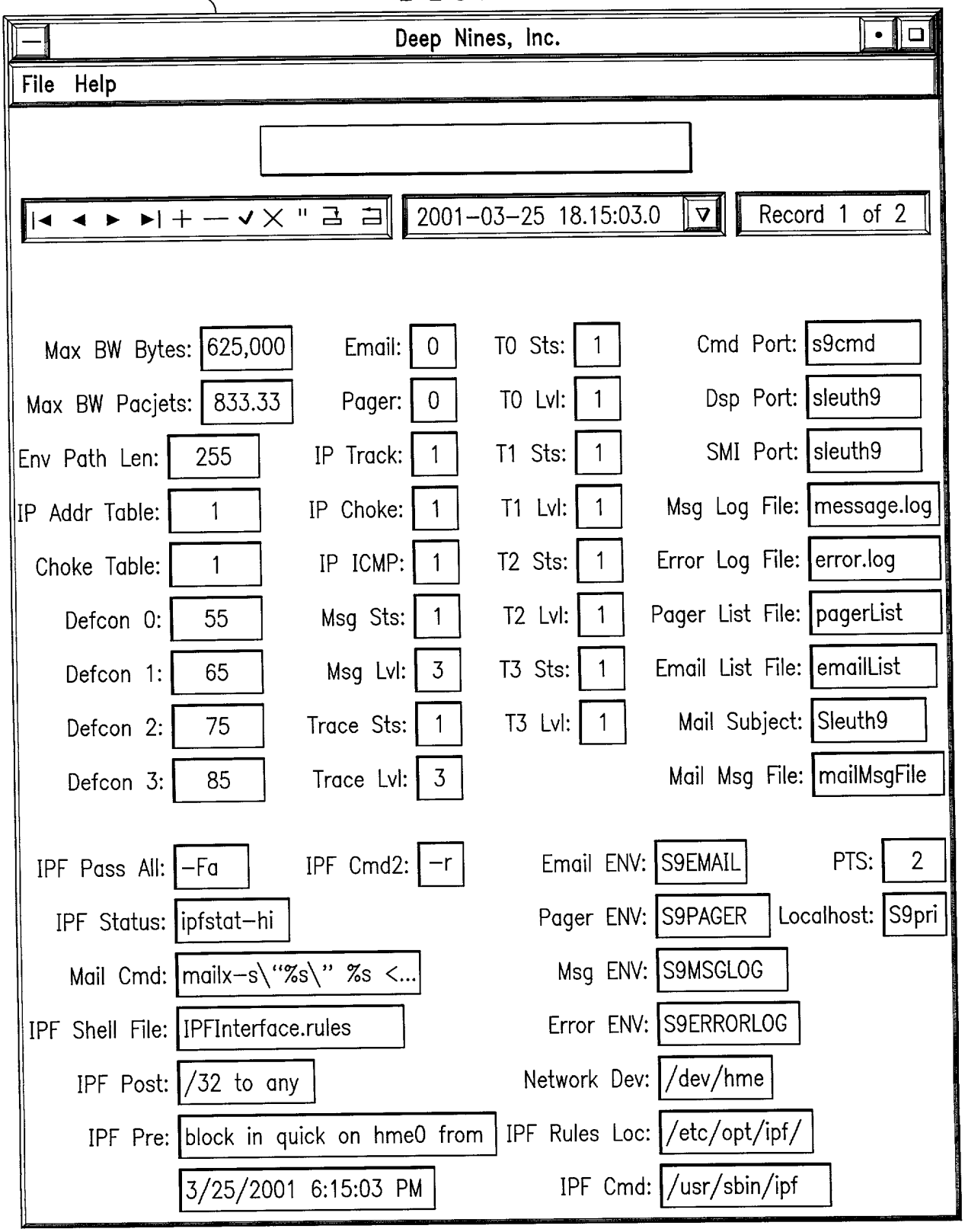

Deep Nines, Inc.
File Help
IP Tracking
Record 1 of 43
701
702
703
704
705
706
BYTES
BYTESPTS
BYTESLASTPTS
ACCUMBYTESLAST
IPDETECTIONDATE
IPLASTNOTICEDATE
1,107,624 40 40 18,107,624 2/14/01 10:14:15 AM 2/14/01 2:37:27 AM
1,074,749 999 999 1,074,749 2/14/01 10:15:01 AM 2/14/01 2:42:15 AM
833,551 41 41 833,551 2/14/01 10:13:46 AM 2/14/01 2:44:55 AM
477,808 71,379 71,379 447,808 2/14/01 10:10:26 AM 2/16/01 10:48:49 AM
300,426 38,015 38,015 300,426 2/14/01 2:30:48 AM 2/14/01 2:30:51 AM
201,787 43,830 43,830 201,787 2/14/01 10:08:36 AM 2/16/01 10:48:34 AM
69,169 2,950 2,950 69,169 2/14/01 10:10:25 AM 2/16/01 10:45:55 AM
54,450 80 80 54,450 2/14/01 11:18:14 AM 2/14/01 12:19:57 PM
52,471 5,665 5,665 52,471 2/14/01 10:08:38 AM 2/16/01 10:48:35 AM
30,118 2,170 2,170 30,118 2/14/01 12:35:00 PM 2/14/01 12:50:22 PM
700
707
708
709
710
711
CHOKEBYTES
CHOKELEVEL
ACTIVE
CHOKESTARTDATE
CHOKEENDDATE
9,325 2 0 2/14/01 10:17:24 AM 2/14/01 10:37:22 AM
40,425 2 0 2/14/01 10:17:30 AM 2/14/01 10:37:22 AM
137,276 2 0 2/14/01 10:17:39 AM 2/14/01 10:37:22 AM
23,336 2 0 2/14/01 10:17:47 AM 2/14/01 10:37:22 AM
1,540 2 0 2/14/01 10:17:52 AM 2/14/01 10:37:22 AM
40 2 0 2/14/01 10:17:58 AM 2/14/01 10:37:22 AM
46,519 2 0 2/14/01 10:18:03 AM 2/14/01 10:37:22 AM
118,529 2 0 2/14/01 10:18:14 AM 2/14/01 10:37:22 AM
148,551 2 0 2/14/01 10:18:21 AM 2/14/01 10:37:22 AM
Record 1 of 166

FIG. 7

800

FIG. 8


Deep Nines, Inc.
File Help
2001-03-25 18.15:03.0
Record 1 of 2
Max BW Bytes: 625,000
Max BW Pacjets: 833.33
Env Path Len: 255
IP Addr Table: 1
Choke Table: 1
Defcon 0: 55
Defcon 1: 65
Defcon 2: 75
Defcon 3: 85
Email: 0
Pager: 0
IP Track: 1
IP Choke: 1
IP ICMP: 1
Msg Sts: 1
Msg Lvl: 3
Trace Sts: 1
Trace Lvl: 3
T0 Sts: 1
T0 Lvl: 1
T1 Sts: 1
T1 Lvl: 1
T2 Sts: 1
T2 Lvl: 1
T3 Sts: 1
T3 Lvl: 1
Cmd Port: s9cmd
Dsp Port: sleuth9
SMI Port: sleuth9
Msg Log File: message.log
Error Log File: error.log
Pager List File: pagerList
Email List File: emailList
Mail Subject: Sleuth9
Mail Msg File: mailMsgFile
IPF Pass All: -Fa
IPF Cmd2: -r
IPF Status: ipfstat-hi
Mail Cmd: mailx-s\"%s\" %s <...
IPF Shell File: IPFInterface.rules
IPF Post: /32 to any
IPF Pre: block in quick on hme0 from
3/25/2001 6:15:03 PM
Email ENV: S9EMAIL
Pager ENV: S9PAGER
Msg ENV: S9MSGLOG
Error ENV: S9ERRORLOG
Network Dev: /dev/hme
IPF Rules Loc: /etc/opt/ipf/
IPF Cmd: /usr/sbin/ipf
PTS: 2
Localhost: S9pri